

Microsoft Active Directory Best Practices

1. Microsoft recommends more than one domain controller to provide automatic failover protection of the directory. When replication is working properly, a failed Domain Controller will NOT prevent users from logging in. Virtualization can be used for the servers, however for proper failover protection; Microsoft recommends not running multiple virtualized domain controllers on the same physical hardware.
2. Access to domain controllers must be protected from physical and network access of unauthorized personnel. Domain Controller traffic from outside a Protected Network should be protected by being sent through an encrypted tunnel.
3. Time is critical to the Active Directory Domain Controller. The Primary Domain Controller Emulator (PDCE) should be the only server in the Domain getting time from an external source. All other Domain members should get their time from Domain Controllers, which get their time from the PDCE.
4. Child Domains should not be used. Child Domains can complicate administration of AD and should be avoided.
5. The Windows Domain Name Server (DNS) should be used. Windows DNS integrates easily with AD, allowing Dynamic DNS (the automatic registration of host records for forward and reverse lookup zones).
6. Services, such as File Services, DHCP, and Web Servers, should not be installed on Domain Controllers. A service that needs to be restarted should not affect the Domain Controller. In addition, some services create security flaws that can have an impact on the Domain Controller.
7. Backup of Active Directory is critical. Replication alone should not be depended on to be the backup. Active Directory is a database that can become corrupted and the corrupt database will replicate to the other Domain Controllers. In addition, if you delete a user or an OU, you can restore it from your backup. A re-created user (even if she has the same name as the original user) is NOT the same user to AD. If an AD user is re-created (as opposed to restored from backup) all rights and permissions to the new user must be reassigned. This backup should include the system state, not just data.
8. Active Directory has added the Recycle Bin feature for Forest Functional Level 2008 R2 and above. The AD Recycle Bin helps minimize directory service downtime by enhancing the ability to preserve and restore accidentally deleted Active Directory objects (users, groups, computers, and entire OUs) without restoring data from backups. This feature MUST be turned on before deleted objects can be recovered, it is not a default. After the Active Directory Recycle Bin is enabled in the environment, you cannot disable it. When the Active Directory Recycle Bin has not been enabled, objects are stripped down and marked Tombstoned. The garbage collection process will delete these objects when the Tombstone Life Time has expired (180 days by default). Restored user accounts automatically regain all group memberships and corresponding access rights that they had immediately before deletion, within and across domains.

Microsoft Active Directory Best Practices

9. A naming convention should be used for users, groups, computers, printers, and shares. Changing conventions (or having a loose convention) is confusing and error prone. Making mass changes to existing conventions is tedious at best.
10. Use Active Directory to manage printers. The tools are built in to the directory software and starting with Windows 2003 R2, users have the ability to install printers themselves without having a technician come to their computer to do it for them (limited to those users who have permissions to print to a particular printer).
11. Limit users to the rights and permissions needed to accomplish their tasks. Users should be able to use the resource or not. They should not be expected to use the 'honor system' when it comes to resources. Rights and Permissions are sometimes used interchangeably but they are not the same.
 - Rights: The ability to perform some action (for example, change system time or log on to a server)
 - Permissions: Access to a folder or file in the file system.
12. Use Active Directory Groups to assign Rights and Permissions. Assigning directly to users may seem more intuitive at first, but as users change responsibilities, leave and/or join the organization it becomes apparent why it is imperative to use Groups to manage user access. Even if the group has only one member, it is still preferred.
13. User (and computers where applicable) should be made members of Global Groups. The Global Groups should then be made members of Domain Local Groups. The Domain Local Groups should be used to assign rights and permissions. Users can be members of multiple Groups.
14. Group Policies are applied to containers (Domains, Sites, Organizational Units (OUs)) but can be filtered by Groups. For example, a Group Policy applied to the Students OU can be filtered to allow only members of the Group named Class2013 to have the Policy applied to them. When using Group Policies, avoid modifying the Default Domain Policy. Create another GPO (Group Policy Object) at the Domain level, assign the appropriate Delegation, and use it. The Default Domain Policy should be left to be used as a template.
15. Deny Permissions should not be used. Denying a User/Group Permission to a resource is, for the most part, the same as not granting Permission. Allowing too many Users/Groups access to a resource and then denying access to a few leads to unexpected results and makes troubleshooting difficult.
16. Active Directory is a database and can be used to hold detailed User and Computer information. It is best suited for information that does not change frequently. An example of a good candidate for storing in Active Directory is the network address of a computer, which should never change unless the network card is replaced. An example of a poor candidate for storing in Active Directory is the currently logged on user, which might change hourly in a computer lab.
17. The depth of the OU structure of the directory should be no more than three levels if possible. Too many levels can lead to potentially slow logons (too many Policy levels) and difficulty troubleshooting.

Microsoft Active Directory Best Practices

18. The use of 'Generic User Accounts' (user1, teacher, student, etc) should be avoided whenever possible. Some use of 'Service Accounts' to automate backups or nightly processes is unavoidable but should be restricted. The use of Managed Service Accounts (Server 2008 R2) and Group Managed Service Accounts (Server 2012) is highly recommended. GMSAs function like computer accounts – no need to change the passwords manually the system does that for you. This is much preferred to using an account with "password never expires" set.
19. A home directory structure of one share point and each user's Home directory inside (staff\userid) rather than using a share for each user (userid) improves recovery. Both directory structures will work, however share permissions are not saved or restored by backup programs and in the event of a recovery/restore event, all user share permissions will need to be re-entered. This could be time consuming depending on how many shares are impacted.
20. Maintain the Forest and Domain Functional Levels at as high a version as possible to be able to take advantage of the new features come out in every new version upgrade.
21. If any of the replicated servers are available, staff can rebuild from the existing surviving server rather than restore from a backup.
22. Recovery using Active Directory procedures is preferable and should be attempted before a restore is attempted. For example, using the Recovery Bin.
23. Never attempt a restore of data older than the tombstone lifetime as it will cause inconsistencies.